Fake CAPTCHA codes, often filled with malware, only make people hate CAPTCHA even more.

Fake CAPTCHAs are tricking users into downloading malware, making people hate them even more.

Nobody likes CAPTCHAs and having to decode garbled words or click on images just to log in or browse the web. They're created for security purposes, but they're still annoying. Now, fake CAPTCHAs are tricking users into downloading malware, making them even more hated.

CAPTCHA isn't always harmless.

Normally, CAPTCHAs are just a waste of time, but they're harmless. However, a new CAPTCHA scam targeting Windows users turns these annoying puzzles into dangerous malware with just a few keystrokes.

While you're busy proving you're not a robot, hackers are using fake CAPTCHA pages to trick you into performing a malware installation task. You still won't be able to access the website you wanted, but the hackers have gained full access to your computer.

These fake verifications look exactly like regular Cloudflare security checks, making it difficult to distinguish between genuine and fake. After all, we've become so accustomed to simply completing the task and moving on without giving any thought to whether the verification is real or fake.

Hackers installed Stealthy StealC malware. It steals login credentials while you're browsing the web, data from cryptocurrency wallets, information from Outlook emails, Steam account information, etc.

Normally, you just need to stay away from suspicious websites and you'll be fine. However, hackers are infiltrating CAPTCHA pages on legitimate websites. A simple piece of malicious JavaScript code replaces the real CAPTCHA with a fake one. This is a form of clickjacking, making legitimate websites suddenly appear

malicious.

Be careful with CAPTCHAs that use keyboard shortcuts.

Typically, CAPTCHA requires you to move a puzzle piece, enter random letters, select a specific image from a set, or solve a simple math problem. These fake CAPTCHAs containing malware do things differently.

They require users to press a series of keyboard shortcuts. A valid CAPTCHA will not require you to enter any shortcuts. In this case, the key combination is **Win + R** to open the Run window in the background. Then, you press **Ctrl + V** to paste the malicious command, even though you can't see it. After that, you are prompted to press Enter **,** which executes the command and downloads the malware.

This isn't the first time this type of attack has occurred, and it won't be the last. Just a year ago, EDDIESTEALER targeted Windows users on Chrome to install malware through fake CAPTCHA pages.

How to distinguish between real and fake CAPTCHA

Most CAPTCHAs you encounter are real. You may not like them, but they are a legitimate verification tool to protect websites from bots. They are becoming more common thanks to artificial intelligence (AI) and the rise of AI-powered web data collection.

Some signs to recognize whether a CAPTCHA is malicious or not include:

1. It requires you to run a script or command.
2. The "I'm Not a Robot" checkbox leads to a list of keyboard shortcuts instead of a challenge like selecting an image.
3. CAPTCHA appears randomly instead of upon login or first-time website visit.
4. The CAPTCHA opens a new page with a slightly altered URL.
5. Strange spacing or grammatical errors in the instructions.
6. Extremely low-quality images require you to use keyboard shortcuts instead of selecting the image.

The article also encourages you to pay attention to what's happening in the background. If you're interacting with a CAPTCHA and see a PowerShell or Command Prompt icon appear on the taskbar, stop whatever you're doing and leave the CAPTCHA page immediately.

Consider disabling scripts in Windows!

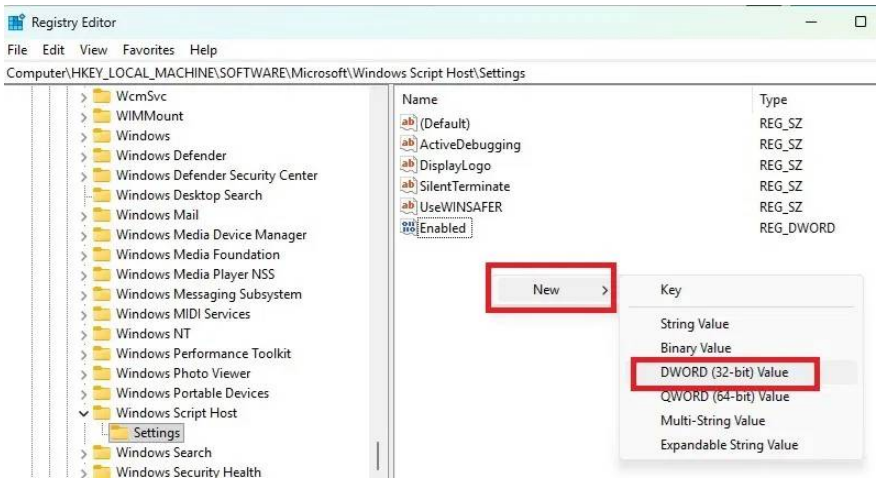
It might seem extreme, but disabling the Windows Script Host helps prevent malicious scripts from running. You can also use a less extreme method to prevent Windows from running any unsigned scripts.

If you have administrator privileges and are comfortable editing the Registry, you can disable Windows Script Host. It's very easy to re-enable it whenever you need to.

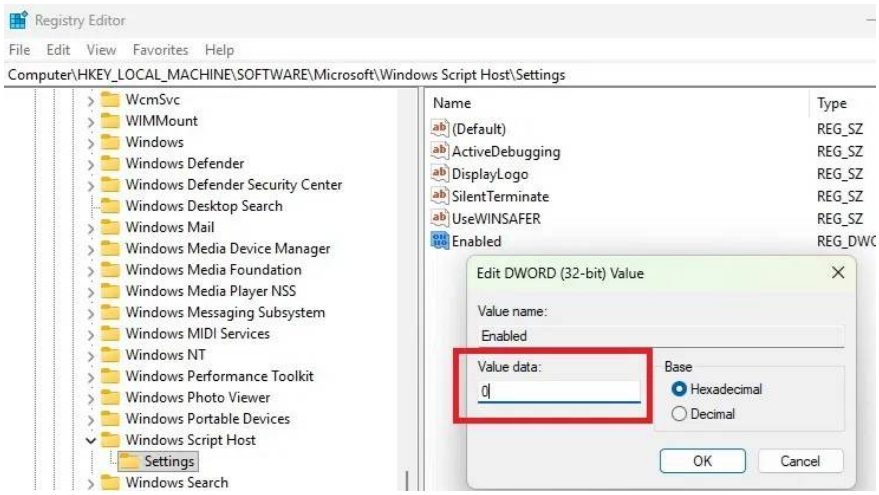
Press **Win + R** , type **regedit** and press **Enter.** Navigate to:

```
HKEY_LOCAL_MACHINESoftwareMicrosoftWindows Script HostSettings
```

Right-click on an empty area in the right pane and select **New ? DWORD (32-bit) Value** .



Name the new value **Enabled** . Double-click the new value and set its value to 0. **Restart** your PC and you're done. If you want to allow scripts, set the value to **1** .



This also blocks legitimate scripts. But re-enabling it is fairly simple.

Block JavaScript on websites.

Another method to prevent CAPTCHA spoofing is to block JavaScript elements on websites. This might break some features on your favorite websites, but you can enable JavaScript for each individual website.

You can find JavaScript settings in your favorite browser's settings. Or, consider using a script-blocking extension like NoScript . Or, try a security and privacy extension like uBlockOrigin to customize what you want to block.

Fake CAPTCHAs won't disappear. But by blocking the scripts from running and paying close attention to the CAPTCHA instructions, you'll have a better chance of avoiding hidden malware.

tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.